

STATE OF OHIO



DEPARTMENT OF REHABILITATION
AND CORRECTION

SUBJECT: Information Technology Systems Password and Account Security	PAGE <u> 1 </u> of <u> 4 </u>
	NUMBER: 05-OIT-17
RULE/CODE REFERENCE:	SUPERSEDES: 05-OIT-17 dated 07/12/12
RELATED ACA STANDARDS:	EFFECTIVE DATE: August 11, 2014
	APPROVED:

I. AUTHORITY

This policy is issued in compliance with Ohio Revised Code 5120.01 which delegates to the Director of the Department of Rehabilitation and Correction the authority to manage and direct the total operations of the Department and to establish such rules and regulations as the Director prescribes.

II. PURPOSE

The purpose of this policy is to establish Department of Rehabilitation and Correction computer user password security requirements to protect State information technology system assets.

III. APPLICABILITY

This policy applies to all Department of Rehabilitation and Correction employees and contractors, including temporary employees that have computer access to State information technology system assets.

IV. DEFINITIONS

Administrative Account – A privileged, higher level information technology system account that permits the account holder to grant system access, levels, rights, permissions and passwords to computer end users.

System Assets – Computer hardware, software, networks, data and/or services or resources that are necessary to support the information technology requirements of the Ohio Department of Rehabilitation and Correction and therefore must be protected by the appropriate security requirements to ensure business continuity.

V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction (DRC) to protect its information technology system assets by establishing and managing security requirements for user passwords and personal user identifiers pursuant to the standards established by the Department of Rehabilitation and Correction Office of Administration, Bureau of Information Technology Services (BITS) and the Ohio Administrative Services, Office of Information Technology (DAS – OIT).

VI. PROCEDURES

A. Password Standards and Administration

1. User password protocols, including access levels, rights, and permissions for Department of Rehabilitation and Correction information technology systems shall be established pursuant to the standards established by BITS and DAS – OIT.
2. The Chief of BITS shall designate BITS staff responsible for managing administrative accounts that define password access levels, rights, and permissions for information technology systems used by a Department of Rehabilitation and Correction employee or contractors.

B. Password and Logon Security

1. User passwords for DRC information technology systems shall meet or exceed the following security standards:
 - a. Minimum of eight (08) characters in length;
 - b. Contain at least one upper case letter;
 - c. Contain at least one special character (e.g. !, @, #, \$, %, ^, &, *);
 - d. Not contain personal user identifiers (e.g. SSN, DOB, telephone number, part of a user name).
2. Smartphones are only required to have a four digit password and are exempt from the complex password requirements established in section B1 of this policy.
3. DRC information technology user accounts for all systems shall be associated with a single individual user and shall not be established for use for multiple users. The combination of a user identification and personal password shall authenticate a unique, individual employee or contractor user account.
4. Pursuant to Department Policy 05-OIT-10, Internet, Electronic Mail, and On-Line Services Use, all employees and contractors with access to DRC information technology systems are prohibited from sharing their unique, individual usernames and passwords with anyone. In addition, they are prohibited from displaying their unique, individual usernames and passwords where others may view them.
5. DRC information technology systems that can automatically compel employee or contractor users to change their individual passwords shall be configured to compel password changes every 90 days.
6. DRC employee and contractor users shall not, under any circumstance, use a “save password” option when using DRC information technology systems to conduct State business.

C. Account Deactivation

1. When a DRC employee is terminated for a violation of the Code of Conduct or is placed on administrative leave for any reason or when a contractor's service is terminated for any reason, all the employee or contractor's information technology system accounts shall be immediately deactivated as follows:
 - a. The employee's supervisor or, in the case of a contractor, the appropriate supervisor designated by the Managing Officer, shall immediately contact the Chief of BITS.
 - b. The Chief of BITS shall direct the appropriate BITS staff members to deactivate all information technology system accounts associated with the employee or contractor.
2. When a DRC employee terminates service or a contractor terminates or otherwise closes a contract with the DRC, all information technology system accounts assigned to the employee or contractor shall be deactivated.
 - a. The employee's supervisor or, in the case of a contractor, the appropriate management employee designated by the Managing Officer shall complete the System Deletion/Deactivation Form (DRC1889) by the end of the business day when an employee terminates employment or, in the case of a contractor, when a contract is terminated or otherwise closed, and submit the completed form to the DRC Information Service Center.
 - b. Upon receipt of the System Deletion/Deactivation Form (DRC1889), the DRC Information Service Center shall immediately deactivate all information technology system accounts associated with the employee or the contractor.
3. When a DRC employee or contractor transfers to another DRC location or is reassigned to another position resulting in a change in job duties, the employee's supervisor, or in the case of a contractor, the appropriate management employee designated by the Managing Officer, shall assess the employee or contractor's access to DRC information technology systems to determine if system access should be modified. If it is determined that system access will be modified:
 - a. The employee's supervisor or, in the case of a contractor, the appropriate management employee designated by the Managing Officer, shall complete the System Deletion/Deactivation Form (DRC1889) and the System Access Request Form (DRC3424) and submit the completed forms to the DRC Information Service Center.
 - b. Upon receipt of the forms, the DRC Information Service Center shall deactivate the appropriate information technology systems accounts identified on the System Deletion/Deactivation Form (DRC1889) and activate the appropriate information technology systems accounts identified on the System Access Request Form (DRC3424).
4. When a DRC employee begins an extended leave of absence (e.g. FMLA, disability, military leave):

- a. The employee's supervisor shall complete the System Deletion/Deactivation Form (DRC1889) and submit it to the DRC Information Service Center by the end of the first business day of the leave of absence so that Information Service Center Staff deactivate all the employee's system accounts.
- b. Upon the employee's return from the extended leave of absence, the employee's supervisor shall ensure the System Access Request Form (DRC3424) is completed and submitted it to the DRC Information Service Center to reactivate the employee's information technology systems accounts.

D. Compromised Passwords

When an employee learns that any of his/her assigned DRC information technology system passwords or accounts have been compromised, the employee shall immediately notify his/her supervisor and complete an Incident Report (DRC1000) pursuant to Policy 01-COM-08, Incident Reporting and Notification.

1. In addition to distributing the Incident Report to the supervisor and other appropriate managers in the employee's chain of command, the employee shall distribute the Incident Report to the Chief of BITS, who shall take the necessary steps to immediately deactivate the employee's DRC information technology system passwords or accounts.
2. Once a decision is made to reactivate the employee's information technology system accounts, the employee's supervisor shall submit a System Access Request Form (DRC3424) to the DRC Information Service Center for reactivation.

Related Department Forms

System Access Request Form	DRC3424
Incident Report	DRC1000
System Deletion/Deactivation Form	DRC1889